
Classification


14 Sept 53

FROM: NSA-41, Mr. Austin

TO: Mr. Friedman

Received 1 copy of the item listed below:

Memo for Members of the U.S. Delegation, dtd 11 Sept 53
Copy No. 16 of TOP SECRET CONTROL NO. 53-41-183



Signature

Classification

~~TOP SECRET~~~~TOP SECRET - SECURITY INFORMATION~~

11 September 1953

MEMORANDUM FOR MEMBERS OF THE U.S. DELEGATION

SUBJECT: UK/US COMSEC Conference

Forwarded herewith is a copy of a UK paper reviewing the present status of UK cryptographic equipments. This is an advance version which has not received final approval and is subject to amendment both before and during the Conference.


FRANK C. AUSTIN

~~TOP SECRET CONTROL NUMBER~~ 5-41-53
COPY 16 OF 20 COPIES
PAGE 1 OF 1 PAGES

~~TOP SECRET~~

~~TOP SECRET~~~~TOP SECRET - SECURITY INFORMATION~~U.K. CRYPTOGRAPHIC EQUIPMENTSPART I. LITERAL CYPHER MACHINES.1. Machine Requiring no External Source of Power.(a) PORTEX.

A small hand operated off-line tape printing cypher machine with an electrical permuting maze designed for low echelon use. Electrical power to operate the maze is derived from a self-contained 45-volt dry battery good for over 100,000 operations. The cryptographic unit consists of an eight 26-point rotor maze with a crossover at the cypher end; the rotors step in two four-rotor cyclometric cascades. Each rotor consists of an insert and a housing; the insert is selected from a set of sixteen and can be fitted in the housing in any one of the twenty-six possible angular positions, the housing is fitted with a rotatable alphabet tyre.

Size of machine: 13" x 9½" x 7½" Weight 22 lbs.

Production State: No orders will be placed until after completion of user trials in September 1953. Production will start eighteen months after placing of firm order.

Security State: At 1952 Conference both U.K. and U.S. agreed that security afforded was inadequate. Since then the crossover has been added and it is now the U.K. view that security is adequate for the purpose envisaged.

2. Power Driven Machines.(a) TYPEX 2.

A power driven keyboard operated tape printing cypher machine with a five 26-point rotor reciprocal permuting maze with a pluggable reflector. Rotors consist of a housing with a rotatable notch ring and alphabet tyre into which can be fitted reversible wired inserts selected from a set of fourteen. Only three rotors turn during the encryption of a message. The cryptogram is arranged in groups of five letters, a check printer is provided.

Size and Weight (in transit case) 3' x 2' x 1' 3" 160 lbs.

Production State: No more of these machines will be manufactured.

Security State: At 1952 Conference it was agreed that used with Simplex (one-time) rotor arrangements and message settings the equipment was secure for Top Level NATO communications.

TOP SECRET CONTROL NUMBER 5-11-53
COPY 11 OF 11 COPIES
PAGE 1 OF 11 PAGES

~~TOP SECRET~~

~~TOP SECRET~~~~TOP SECRET - SECURITY INFORMATION~~(b) TYPEX 22.

The general purpose U.K. cypher machine; similar to the Typex 2 except that all rotors turn during the encryption of a message and a pluggable crossover is provided at the entry (and exit) to the mazes.

Security State: U.K. view is that the machine is secure for all classifications of traffic provided bisection and variable spacing are employed. There is no U.S. assessment.

(c) FORTEX IIA.

A keyboard operated motor driven version of the FORTEX I. Operating speed 130 characters per minute.

Status: One development model constructed. Adoption of the machine depends upon policy for the adoption of FORTEX I.

(d) SINGLET.

A keyboard operated motor driven tape printing cypher machine having a ten 36-point rotor non-reciprocal permuting maze using re-entry technique with a pluggable crossover at the cypher end. The keyboard will provide for the encryption of the full combined teleprinter alphabet as laid down in ACP 126 plus the punctuation marks, comma, colon, question mark, quote mark. In addition, the letters J and Z will be recovered in the upper case and facilities will be provided for encrypting carriage return and line feed. The cryptogram will consist of letters arranged in groups of five; a check printer will be provided. Inter-operation with AFSAM 7 and PENDRAGON will be possible.

Estimated size and weight: 2½ cu.ft. 75 lbs.

Status: A model to comply with the latest specification (agreed in April 1953) due for demonstration March 1954.

(e) PENDRAGON.

Major office variant of SINGLET. Operates automatically from tape input and designed for use with both one-wire and five-wire teleprinter ancillary equipments. Will interwork with SINGLET and AFSAM 7.

Estimated size and weight: 3 cu.ft. 100 lbs.

Status: A model to comply with latest specification (agreed in April 1953) due for demonstration June 1954.

2

TOP SECRET CONTROL NUMBER 500 11-1
 COPY 16 OF 20 COPIES
 PAGE 2 OF 12 PAGES

~~TOP SECRET~~

~~TOP SECRET~~~~TOP SECRET - SECURITY INFORMATION~~PART II. TELETYPE TELEPRINTER SECURITY EQUIPMENTS.3. Non-Synchronous with Electro-mechanical Crypto-Components.(a) MINSTER.

Interim equipment for on-line non-synchronous (start-stop) point to point usage over wire circuits. Half-duplex operation. Crypto-component is a rotor maze generating additive key using six 31-point double rotors. Maze steps at alternate encypherments.

Estimated Size and Weight: 2' x 2' x 3" 150 lbs.

Development Status: Development complete. Placing of contracts awaits clarification of user requirements.

Security Status: At 1952 Conference U.K. stated security acceptable for intended purpose, U.S. required further study.

[NOTE: Possibility of re-designing MINSTER with a permuting maze and 32 or 36 point rotor is under investigation.]

4. Non-Synchronous with Electronic Crypto-Component.(1) PHILOMEL (modified ROLLICK).

Non-synchronous equipment using subtractor (additive) key derived from an electronic key generator (single TUTTE) employing multi-cold-cathode tubes. Cypher setting is changed by means of plugs and counter settings at the beginning of each day and after outage; to minimize the number of reset operations a character counting device is to be fitted to enable operators to regain synchronism on the original key cycle following temporary loss due to line faults and operator errors. This new method of resetting replaces the random generator setting. To limit the dangers of insecure radiation the equipment is being arranged to be capable of use on either a d.c. or a tone-keying basis. The equipment can be remotely controlled from the teleprinter position.

Size and Weight: 4' 6" x 19" x 12" 250 lbs.

Development Status: Contract for 115 equipments placed and due for completion May 1954. The first 50/60 will require retrospective action to incorporate the character counter and tone-keying modifications.

Security Status: U.K. view is that the equipment is secure for use over wire circuits on which there is little chance of continuous interception of the transmitted signal by potentially enemy personnel and provided the plug and counter settings are changed at every reset. U.S. require further study.

TOP SECRET CONTROL NUMBER

COPY 14 OF 100 COPIES
PAGE 4 OF 10 PAGES~~TOP SECRET~~

~~TOP SECRET~~~~TOP SECRET SECURITY INFORMATION~~5. Synchronous Equipment with Electro-Mechanical Crypto-Component.(a) Circuit Mercury.

Single channel duplex, synchronous equipment operating at rates of 45 or 50 bauds. Accepts 31 characters (excluding blanks) from remote teleprinters. Does not provide traffic flow security. Crypto-component consists of two rotor mazes, one with six 31-point double rotors for encypherment and the other with four 31-point double rotors for motion control. Uses relay 5/32 translators. Used by the Air Ministry over long-distance radio teleprinter circuits.

Size and Weight: Two 2' x 2' x 3' consoles and one 6' x 19" rack per duplex terminal. Wt. approx. 400 lbs.

Status: In use and in production.

Security Status: At 1952 Conference both U.K. and U.S. agreed the equipment was secure for traffic of all classifications. Authorized for passing NATO traffic.

(b) Apparatus 5 UCO Single Channel No. 1.

Single channel duplex synchronous equipment using random one-time five unit tape for cypher key. Accepts 31 characters (excluding blank). By using a magnet operated tape reader, facilities for the encryption of all 32 teleprinter characters can be provided. Designed to give traffic flow security but this facility has recently been found to be inadequate and a modification unit is being designed to rectify this deficiency. Equipment is used on long-distance telegraph circuits over radio and wire when the transmission error rate renders start-stop equipment unsatisfactory.

Size: One 6' x 19" double sized rack per duplex terminal.

Status: In use and in production at rate of six equipments per month. Existing orders will be completed early in 1954.

Security Status: At 1952 Conference both U.K. and U.S. agreed that the equipment was secure for all classifications of traffic subject to adequate checks of the standard of the one time tape. Released for use by NATO countries subject to adequate safeguards against insecure radiation.

6. Synchronous Equipments with Electronic Cryptographic Component.(a) ARTICHOKE.

Twin channel duplex synchronous system using subtractor (additive) key derived from an electronic key generator (double TUTTE) employing multi-cold-cathode tubes. Accepts 31 characters (excluding blanks) from remote

TOP SECRET CONTROL NUMBER 2-11-11
 COPY 16 OF 25 COPIES
 PAGE 7 OF 12 PAGES

~~TOP SECRET~~

~~TOP SECRET~~~~TOP SECRET - SECURITY INFORMATION~~

start/stop teleprinter ancillaries or 32 characters from tape. Operates at 50 or 75 bauds, and provides traffic flow security. Basic cypher setting of each key generation achieved by means of 27 chosen from a set of 80, subsidiary setting controlled by a quasi random setting of the counter and 64 position cyclometer switch which is advanced one position for each reset. Plugs are changed completely after every 64 resets. To be employed on long distance radio and wire teleprinter circuits.

Size: One 7' x 19" double sided rack per twin channel duplex system. For vehicle installation the equipment can be mounted on one double-side 5' 3" rack and one single sided 4' 8" rack.

Status: Engineering ("A") model demonstrated in 1952. Service trials of manufacturers ("B") models due for completion by October 1953; production at 6 per month due to start July 1954.

Security Assessment: At the 1952 Conference U.K. assessed the equipment as secure for combined communications; U.S. required further study.

(b) Convertor No.5.

Key Tape Eliminator for use with Apparatus 5 UCO. Consists of an electronic key generator (double TUTTE) similar to that used in ARTICHOKE. The setting of the key generator is identical to that in ARTICHOKE except that the quasi-random setting of the counter is replaced by counter setting according to key lists. Synchronous operation is derived from the Apparatus 5 UCO, traffic flow security is provided. Slightly modified the equipment can be used independently as a self-contained start/stop on-line teleprinter cypher device.

Size: One single sided 6' rack, but probably with auxiliary unit for start/stop.

Status: Development models due for completion September 1953.

Security Assessment: U.K. view is that equipment is secure for use on point-to-point circuits for traffic of all classifications. U.S. require further study.

7. Self-Synchronising and Autoclavic Equipment.

(a) INCUBATOR (late CHEAPEX)

A start/stop cypher text auto key over/over Simplex teleprinter cypher device. The object of the device is to provide the maximum security at a minimum cost and to this end the increased error rate inherent in a self-synchronising system of this type is to be investigated - the delay line from which the cypher key is derived is forty elements long. A transmission error may cause an extended garble. The garble feature limits the use of the equipment to good quality wire and radio circuits.

TOP SECRET CONTROL NUMBER 55-11-18
COPY 16 OF 51 COPIES
PAGE 6 OF 10 PAGES

~~TOP SECRET~~

~~TOP SECRET~~~~TOP SECRET - SECURITY INFORMATION~~

Size: Not yet determined.

Status: Two breadboard models are due for completion in August 1953, magnetic binary circuits are being employed for the delay line and hard valves for the remainder of the equipment. These equipments will be used to determine whether the garble feature can be accepted in practice.

Security Status: The U.K. consider that with minor modifications, the equipment as being developed will give adequate security for the next five years for traffic passed over low echelon networks of classifications up to and including Top Secret.

8. Off-Line Equipment.

(a) ROCKEX.

An off-line teleprinter cyphering equipment using a six unit one time key tape. Accepts 31 characters and by means of an electronic stunt suppression unit produces an all-letter cryptogram in five letter groups, ten groups to the line and five lines to a paragraph. A new unencyphered sequential indicator is used at the beginning of each paragraph. Operates at either Creed or Teletype speed. 5-wire and electronic versions have been produced for use where there is a danger of interception of radiated plain text signals.

Status: In use and in production.

Security Status: At 1952 Conference UK and US agreed that the equipment was secure for the encyphermant of traffic of all classifications subject to adequate security checks during the manufacture of the one-time key tape.

PART III. SPEECH SECURITY EQUIPMENTS.

9. Vocoder Systems.

(a) BANGLE.

Single channel duplex fixed plant speech security system for use over land line or long distance HF radio. Requires one 5 Kc or two 3 Kc transmission channels. Uses a 12 channel vocoder (10 spectrum and 2 independent pitch channels each quantized into 9 levels). Crypto-component consists of 12 independent random keys furnished on 35 mm. film. Tube complement approximately 2000.

Size and Weight: 14 bays of equipment either fixed plant or 3 special vehicles.

Status: Land-line trials carried out in U.K. over period March-July 1953. Radio trials scheduled for early 1954. Only four equipments to be completed; size, weight and administrative problems preclude general adoption of this equipment.

TOP SECRET CONTROL NUMBER
COPY 16 OF COPIES
PAGE 7 OF PAGES

~~TOP SECRET~~

~~TOP SECRET~~~~TOP SECRET - SECURITY INFORMATION~~

Security Status: At 1952 Conference U.K. and U.S. agreed that equipment is secure provided key film is subjected to adequate checks during manufacture.

(b) SORCERER.

Single channel full duplex speech security equipment for use over land lines, short and long haul radio circuits. Uses nine channel vocoder (8 spectrum and 1 pitch). Crypto-component will be Converter No.5 supplying additive key.

Status: Two models for demonstration on a back-to-back basis, each consisting of four racks of equipment are due for completion in Autumn 1953. It is hoped that the final model will be considerably smaller.

Security Assessment: The U.K. view is that the equipment is secure for its intended use. The U.S. require further study.

10. Directly Quantised Systems.(a) BLUE BOY (D.70)

Twelve channel full duplex microwave radio relay speech security equipment. Twenty-four teleprinter channels may be furnished by time multiplexing in lieu of one telephone channel. Speech channels are quantised to 32 PCM levels. Each channel is sampled 7000 times per second, resulting in a total rate of 420 kilobands. Employs an electronic key generator (TUTTE).

Status: Two repackaged development models of the key generator due for completion by end of 1953.

Security Status: U.K. view is that the equipment is secure for its intended use subject to a review in five years. U.S. require further study.

(b) TRUMPETER. A development project whose ultimate aim is to provide a low echelon airborne or ground push-to-talk speech security equipment. The crypto-component will consist of a cypher text auto-key device. The method of speech coding is not yet decided.

Status: In the early development stage. A first development model of the key generator employing gas tubes due for completion October 1953.

Security Status: U.K. view is that subject to the incorporation of certain modifications in the production model of the key generator, the equipment will be secure for the encypharment of low echelon traffic for the next five years. U.S. require to study the proposal.

TOP SECRET CONTROL NUMBER
 COPY 8 OF 6 COPIES
 PAGE 7 OF 12 PAGES

~~TOP SECRET~~

~~TOP SECRET - SECURITY INFORMATION~~~~TOP SECRET~~(c) HALLMARK II.

Single channel, self-synchronous push-to-talk speech security equipment. Speech is sampled at 33.3 Kc. rate and is quantized by a delta modulation scheme. Noise is injected along with its speech input. Encypherment is provided by three auto-key stages in cascade. The equipment is primarily designed for use over tactical line of sight radio circuits. Alternative methods of operation are possible.

- (1) Line of sight radio: Push to talk keyer at each terminal.
- (2) Special wire lines (4 wire): Full duplex with different keyers at each terminal for send and receive.
- (3) When additional security is required for line or radio: Full duplex or push to talk with two keyers in series at each terminal for each direction of transmission.

Size and Weight: Delta modulator 20" x 16" x 14" 80 lbs.
Each keyer unit 20" x 16" x 14" 107 lbs.

Production Status: Production prototype models due for completion Summer 1953. Production of sufficient models to permit full scale troop trials due to start 1954.

Security Status: U.K. consider equipment gives adequate security for point-to-point low echelon use. The U.S. requires further study. When two key generators are used in series much higher security is provided.

(d) PICKWICK.

A single channel duplex ciphony system for use on special land lines. Its primary function is on short distance circuits between special subscribers within, say, the London area. Speech input is Delta pulse code modulated with sampling rate of 15,000 per second. Binary cypher key is derived from 4 self-synchronous HALLMARK II style rings of length 32. Transmission system will probably be 4 level at 7,500 bauds.

Size: One 6' rack (double sided)

Production Status: Two development models due for trial August 1953.

Security Status: U.K. assessment incomplete. U.S. will require study.

PART IV. FACSIMILE SYSTEMS.11. MOUNTBANK (late METFAX)

A system for the encyphered transmission of black and white meteorological charts and similar data. Transmitted signal when in single channel binary form is at about 1,000 bauds. Designed for use with standard

CONTROL NUMBER 5-41-18
COPY 14 OF 20 COPIES
PAGE 7 OF 10 PAGES

8
~~TOP SECRET~~

~~TOP SECRET~~~~TOP SECRET - SECURITY INFORMATION~~

facsimile equipment and to meet a requirement to transmit charts 20" x 16" in not more than 30 minutes with a definition of 100 lines per inch. Cryptocomponent supplies additive binary key derived from an electronic key generator (TUTTE). The method of starting the key generator in step is a frame synchronising system similar to that used in ASAY 8 (X-3).

Size: 2 racks 6' x 20" (1 encypher, 1 decypher)

Status: Trials using development models being carried out over radio during the period July to December 1953.

Security Status: U.K. view is that the equipment is secure for its intended use. U.S. require further study.

PART V. CRYPTOLOGIC EQUIPMENTS.

12. One-Time Pad Production Equipment.

(a) TRIMMER.

Represents the first effort towards utilising electronically generated random signals for the production of one-time pads. Source of signals is an electronic randomizer similar to that used in several other applications (e.g. 5 UCO key tape). Output is printed on wide carriage electromatic typewriters. Format programming is controlled by a unit using new type rotary line finder telephone switches.

Status: One multiple equipment operating five independent outputs has been constructed. Method of bringing it into operational use is being studies.

Security Status: U.K. view is that subject to adequate checks of the output the equipment is secure for its intended purpose.

13. One-Time Tape Production Equipments.

(a) ROCKEX KEY GENERATOR.

Equipment for producing randomly perforated five-level tape. Source of random input signal is an unstable multi-vibrator requiring critical adjustment. A separate source is provided for each stream of holes in the tape. Paragraphing is punched into the tape and is accomplished by the paragraphing unit.

Status: Equipment currently in use and adequate supplies exist. No further production contemplated.

Security Status: Subject to adequate checks of the tape during production the equipment is considered secure by both U.K. and U.S.

~~TOP SECRET~~

~~TOP SECRET~~~~TOP SECRET - SECURITY INFORMATION~~(b) 5 UCO KEY GENERATOR.

Equipment for producing randomly perforated five-level tape with same type of randomizer as used in TRIMMER. A pulse generator is used to time the random source from the reperforators which are free running with clutch locked out. Perforator operating speed is 400 characters per minute (same as rate of usage).

Status: 200 produced. No further production contemplated.

Security Status: Subject to adequate checks of the tape during production the equipment is considered secure by both U.K. and U.S.

14. 5 UCO Tape Checking Equipment.High Speed Checker.

Electronic, high speed checker for 100,000 character spools of random tape used in the Apparatus 5 UCO No.1. Makes the following counts and prints out the results:-

- (1) Plain stream (5 counts)
- (2) Delta streams (5 counts)
- (3) Combinations 1 and 2, 2 and 3, 3 and 4, 4 and 5, 1 and 3, 2 and 4, 3 and 5, 5 and 1 (eight counts).
- (4) 15 consecutive dots in delta stream (5 counts)
- (5) 3 consecutive strikes in delta characters (1 count)

Status: Three equipments built, fourth in course of construction.

PART VI. NEW IDEAS.15. I.F.F. Mk. X. Code Changer for Mode I.

This is a small mechanical 26 point maze of 5 rotors. It is driven by a clockwork clock and the drums move at the code changing interval. It has not been finally decided whether this will be 5 mins. or 15 mins. The maze has a 5 wire output to produce the 5 unit binary codes required. It is used at ground radar I.F.F. interrogators and in airborne transponders.

Target size and weight: As small and light as possible. In practice it may be a cylinder 4¹¹/₁₆" Dia. and about 7¹¹/₉" long. Pressurised. Wt. under 10 lbs.

10

~~TOP SECRET CONTROL NUMBER~~ 27111
 COPY 11 OF 1 COPIES
 PAGE 11 OF 1 PAGES

~~TOP SECRET~~

~~TOP SECRET~~~~TOP SECRET - SECURITY INFORMATION~~

Development Status: First development models should be available mid 1953, but clock may be later.

Security Status: U.K. consider it cryptographically adequate for its function. Main security issues are not cryptographic and involve basic I.F.F. Mk. X programme.

~~TOP SECRET CONTROL NUMBER~~
COPY 16 OF 20 COPIES
PAGE 1 OF 7 PAGES

~~TOP SECRET~~